Microsoft

Microsoft Cloud Compendium

Compliance in der Microsoft Enterprise Cloud

Veröffentlicht von Microsoft Law and Corporate Affairs (LCA) Deutschland
Stand: Juni 2014

Compliance in der Microsoft Enterprise Cloud

Veröffentlicht von Microsoft Law and Corporate Affairs (LCA) Deutschland
Stand: Juni 2014

Wo werden Daten in der Microsoft Enterprise Cloud gespeichert?

Für deutsche Kunden werden standardmäßig die wesentlichen Kundendaten (Core Customer Data) der Microsoft Enterprise Services (Office 365, Microsoft Azure, CRM Online, Windows Intune) in den Microsoft Rechenzentren in Dublin und Amsterdam gespeichert. Microsoft verfolgt bei den Rechenzentren eine an den Regionen orientierte Strategie. Das Land oder die Region des Kunden, das oder die der Administrator bei der erstmaligen Einrichtung der Dienste eingibt, bestimmt den primären Speicherort für die Daten des Kunden.

Die Anforderungen zur Bereitstellung der Dienste können im Einzelfall beinhalten, dass einige Daten Mitarbeitern bzw. Zulieferern von Microsoft außerhalb der primären Speicherregion zugänglich gemacht werden. Darüber hinaus kann es vorkommen, dass sich die Mitarbeiter mit der meisten technischen Erfahrung für die Behandlung spezieller Dienstprobleme an anderen Standorten als am primären Standort befinden, und sie benötigen ggf. Zugriff auf Systeme oder Daten, um das Problem lösen zu können. Dieser Zugriff ist durch die EU Standardvertragsklauseln rechtlich abgesichert.

Microsoft hat derzeit kein deutsches Rechenzentrum. Kann ein deutscher Kunde trotzdem datenschutzkonform Microsoft Enterprise Cloud Services nutzen?

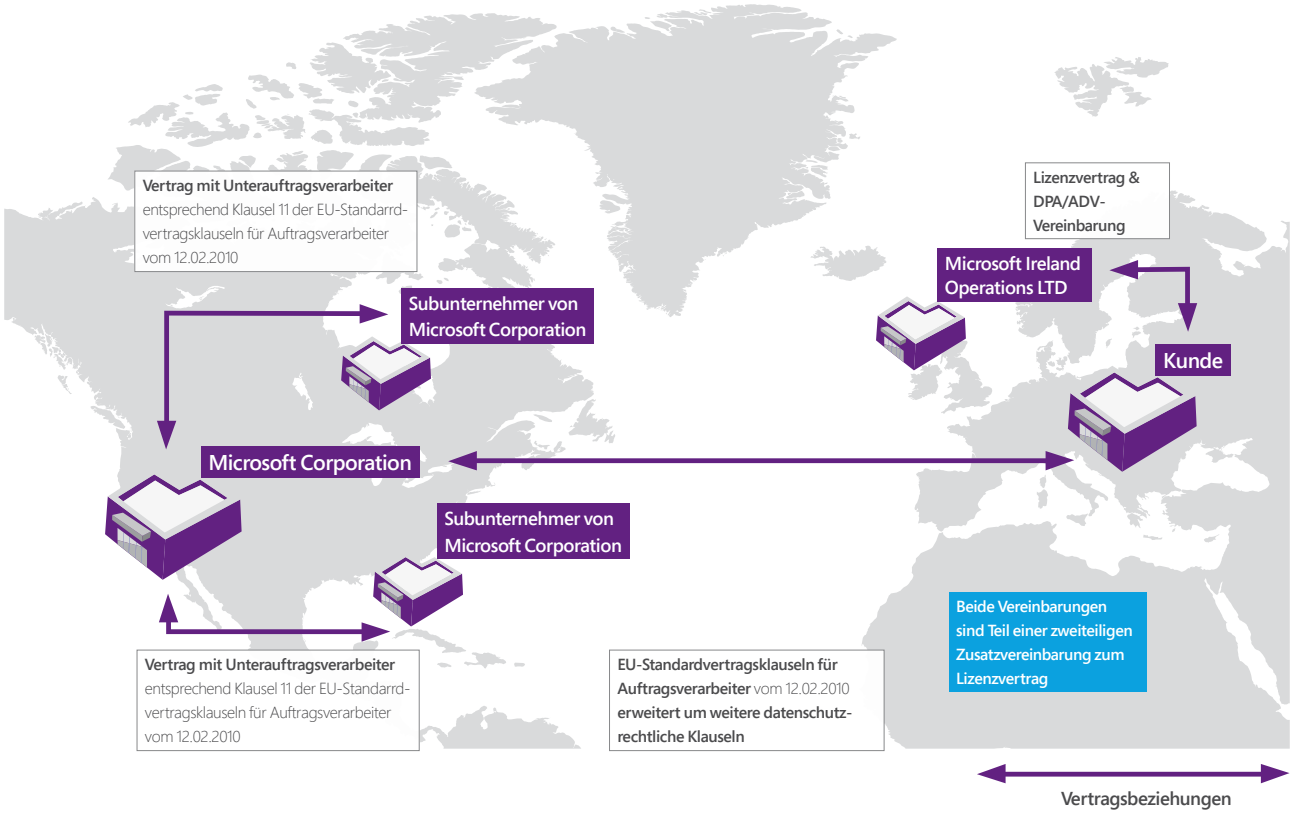
Ja. Rechenzentren in anderen EU-Ländern sind Rechenzentren in Deutschland datenschutzrechtlich gleichgestellt. Dies folgt aus der Waren- und Dienstleistungsfreiheit in der Europäischen Union. Die Dienstleistungsfreiheit ist eine der vier Grundfreiheiten des Europäischen Binnenmarktes. Sie ermöglicht Anbietern den freien Zugang zu den Dienstleistungsmärkten aller Mitgliedstaaten der Europäischen Union. Für den Teil der Services, die Microsoft von außerhalb der EU erbringt, bietet Microsoft seinen Kunden die EU Standardvertragsklauseln an, die eine adäquate datenschutzrechtliche Lösung hierfür sind.

Auf welcher rechtlichen Grundlage verarbeitet Microsoft personenbezogene Daten in ihren Enterprise Cloud Services?

Grundlage für die Leistungsbeziehung sind die Serviceverträge über die Nutzung der jeweiligen Microsoft-Technologie. Diese werden zwischen dem Kunden und der Microsoft Ireland Operations Limited, Irland (nachfolgend: MIOL) abgeschlossen. Die Microsoft Corp, wird dabei als Subunternehmerin von MIOL tätig. Die Serviceverträge werden durch einen Datenverarbeitungsvertrag ergänzt, der die Regelungen für eine Auftragsdatenverarbeitung gemäß § 11 Bundesdatenschutzgesetz BDSG (bzw. den jeweiligen spezialgesetzlichen Vorschriften) enthält.

Der Datenverarbeitungsvertrag enthält als Anhang die EU-Standardvertragsklauseln, die zwischen dem Kunden und der Microsoft Corp. abgeschlossen werden. Die EU-Standardvertragsklauseln sind von der EU-Kommission verabschiedet worden und gewährleisten, dass die Daten bei der Microsoft Corp. nach EU-Datenschutzstandards verarbeitet werden. Sie verpflichten die Microsoft Corp., die EU Datenschutzstandards auch etwaigen Subunternehmern vertraglich aufzuerlegen.

Grafisch stellt sich das Vertragskonstrukt wie folgt dar:



Ändert sich etwas an den Vertragsbeziehungen, wenn die Cloud-Services von verschiedenen Konzerngesellschaften des Kunden genutzt werden?

Die Services können weiterhin von einer zentralen Konzerngesellschaft, beispielsweise der IT-Dienstleistungsgesellschaft des Konzerns, bezogen werden. Der Servicevertrag wird zwischen dieser Konzerngesellschaft und MIOL abgeschlossen. Die EU-Standardvertragsklauseln und die Auftragsdatenverarbeitungsvereinbarung (ADV-Vereinbarung bzw. Data Processing Agreement (DPA)) sollten auf Kundenseite alle nutzenden Konzerngesellschaften unterzeichnen. Diese sind aus Sicht der Datenschutzaufsichtsbehörden die sogenannten verantwortlichen Stellen, die die unmittelbare Vertragsbeziehung zu der nicht in der EU ansässigen Microsoft Corporation haben sollen. Hierfür bietet Microsoft eine Zusatzvereinbarung an.

Welchen Inhalt haben die Vertragsbeziehungen, wenn Unternehmen eine Microsoft-Plattform wie Microsoft Azure nutzen und darauf aufbauend Services ihren Kunden anbieten? [möglicherweise nur für Partner relevant]

Beim sogenannten „Platform as a Service" (PaaS) hängt die Vertragsgestaltung vom Einzelfall ab. Sofern der Microsoft Partner die von ihm entwickelten Applikationen als Service anbieten möchte, ist es zweckmäßig, dass er insofern in seinen Vertragsbedingungen die Maßgaben von Microsoft berücksichtigt, weil er nur die Leistungen weitergeben kann, die er selbst bezieht.

Sind die Enterprise Cloud-Verträge von Microsoft mit den Datenschutzaufsichtsbehörden abgestimmt?
Ja. Die Artikel 29-Datenschutzgruppe, ein Abstimmungsgremium aller 28 nationalen Datenschutzaufsichtsbehörden der EU Mitgliedstaaten, hat Microsoft mit Schreiben vom 2. April 2014 bestätigt, dass das vorgelegte Microsoft-Vertragswerk eine ordnungsgemäße Umsetzung der EU Modell Clauses ist und damit ein angemessenes Datenschutzniveau bei Empfängern außerhalb der EU herstellt (Ref. Ares(2014)1033670 - 02/04/2014) (http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf). Die Datenschutzbehörden haben damit festgestellt, dass das Vertragswerk alle Inhalte aufweist, die für eine weisungsgebundene Beauftragung von Dienstleistern erforderlich ist. Für Unternehmen in Deutschland bedeutet dies, dass die Nutzung nicht durch die Aufsichtsbehörden genehmigt werden muss.

Die letzte Änderung (ein fester Zeitrahmen, in dem die Kundendaten nach Vertragsbeendigung gelöscht werden müssen) ,die Microsoft mit den Datenaufsichtsbehörden abgestimmt hat, wird zum 1.7.2014 in die Standardverträge aufgenommen. Altverträge können aktualisiert werden.

Welche Rolle spielt vor dem Hintergrund dieser Bestätigung noch die Safe Harbor Zertifizierung der Microsoft Corporation für deutsche Kunden?
Es gibt weiterhin Enterprise Cloud Services, für die die Standardvertragsklauseln noch nicht gelten (z.B. Yammer). Für diese Services ist die Safe Harbor Zertifizierung weiterhin von Bedeutung.

Können US-Behörden, wie die National Security Agency (NSA), auf die Daten der Kunden in der Microsoft Cloud zugreifen?
Sollte Microsoft eine Aufforderung zur Herausgabe von Daten erhalten, wird Microsoft den Behörden keine Daten zur Verfügung stellen, sondern die anfordernde Behörde direkt an den Kunden verweisen. Sollte die Behörde gleichwohl die Herausgabe der in den EU-Rechenzentren gespeicherten Inhaltsdaten verlangen, wird Microsoft hiergegen gerichtlich vorgehen, weil die US-Gesetze nach Auffassung von Microsoft nicht für solche Sachverhalte außerhalb der EU gelten. Microsoft hat in diesem Zusammenhang ein Anfechtungsverfahren gegen die von einem US-Richter angeordnete Herausgabe von Daten, die in der EU gespeichert sind, initiiert. Das erstinstanzliche Urteil hat zwar bestätigt, dass Microsoft zur Herausgabe der Daten verpflichtet ist, allerdings wird Microsoft den weiteren Rechtsweg bestreiten, da unseres Erachtens diese Herausgabe nicht rechtmäßig ist. Nähere Einzelheiten hierzu finden Sie hier:

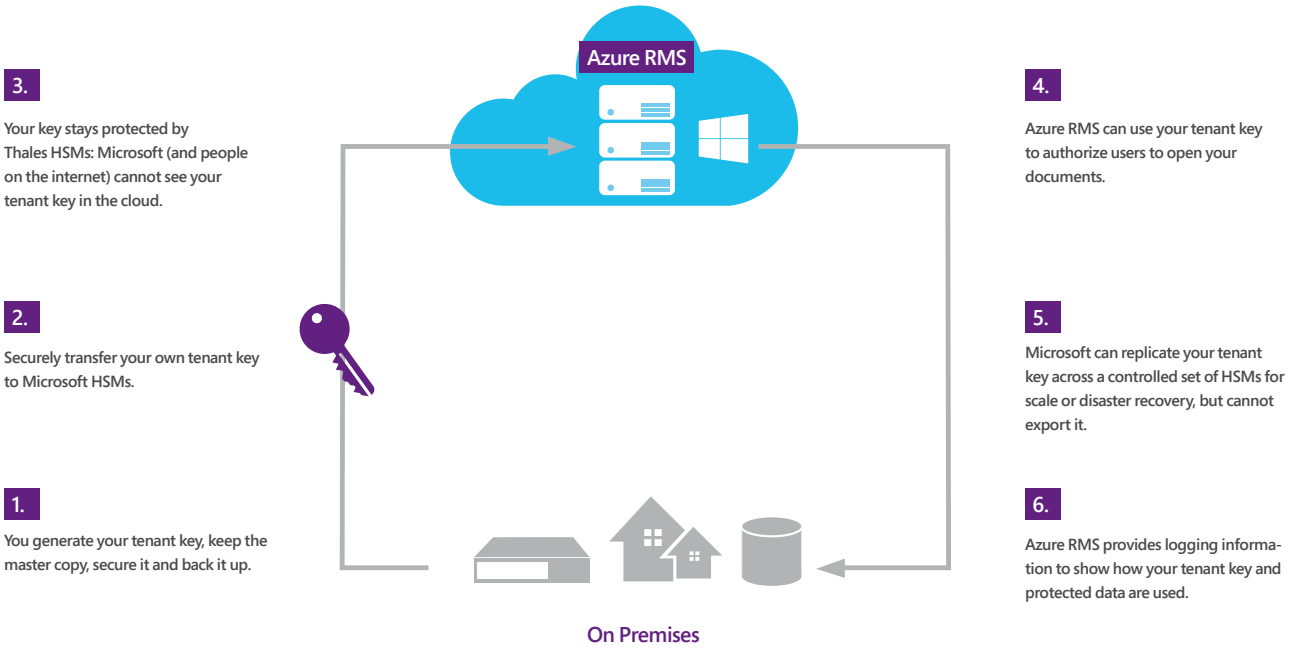
http://blogs.technet.com/b/microsoft_on_the_issues/archive/2014/04/25/one-step-on-the-path-to-challenging-search-warrant-jurisdiction.aspx

Bis zur Erstellung dieses Dokuments gab es im Übrigen noch nie den Fall, dass die NSA von Microsoft die Herausgabe von Daten von Unternehmenskunden verlangt hat.

Kann die Anwendbarkeit des Datenschutzrechts durch Verschlüsselung ausgeschlossen werden?
Dies hängt vor allem von der Art und Weise der Verschlüsselung ab. Sofern eine Verschlüsselung sowohl auf dem Transportweg zwischen Kunde und Microsoft als auch der gespeicherten Daten in der Cloud erfolgt und der Schlüssel allein beim Kunden liegt, fehlt es bereits an der Übermittlung personenbezogener Daten. Eine solche Verschlüsselung kann jedoch die Funktionalität, wie die Suchfunktion, einschränken. Es werden außerdem immer Daten wie die Admin- bzw. Metadaten entstehen, die nicht verschlüsselt werden können, so dass zumindest insofern das Datenschutzrecht zu beachten ist. In jedem Fall ist eine Verschlüsselung ein datenschutzrechtlich positiv zu bewertender Schutz.

Microsoft übermittelt Daten zwischen seinen Rechenzentren daher auch ausschließlich verschlüsselt. Weiterhin bietet Microsoft seinen Kunden an, ihren eigenen Schlüssel für die Verschlüsselung von Daten in Windows Azure Rights Management zu verwenden. Dabei wird der Schlüssel durch ein Hardware-Sicherheitsmodul (HSM) des Hersteller Thales geschützt, so dass Microsoft den Schlüssel nicht exportieren und weitergeben kann.

Grafisch stellt sich dieser Schutz wie folgt dar:



Wie können Kunden ihrer Pflicht nachkommen, sich von der Einhaltung aller technischen und organisatorischen Maßnahmen zu überzeugen?

Microsoft lässt seine Systeme von Drittanbietern prüfen und zertifizieren, damit alle Kunden darauf vertrauen können, dass die Dienste mit strengen Schutzvorrichtungen entwickelt und ausgeführt werden. Wir haben geeignete technische und organisatorische Maßnahmen, interne Kontrollen und Informationssicherheitsroutinen eingeführt und halten diese aufrecht, um Kundendaten vor unbeabsichtigtem Verlust, Zerstörung oder Änderung, nicht autorisierter Weitergabe oder unberechtigtem Zugriff sowie gesetzeswidriger Zerstörung zu schützen. Jedes Jahr unterziehen wir uns Überwachungen durch Dritte, die von international anerkannten Überwachungsinstitutionen ausgeführt werden und bei denen von unabhängiger Seite überprüft wird, ob wir die Einhaltung unserer Richtlinien und Verfahren für Sicherheit, Datenschutz, Kontinuität und Konformität gewährleisten.

ISO 27001 ist hier einer der besten globalen Sicherheitsvergleichs-Benchmarks. Microsoft stellt seinen Kunden einen Bericht nach dem Standards ISO 27001 zur Verfügung. Der Kunde kann diesen Bericht anfordern.

Wie kann der Kunde seine Daten revisionssicher aufbewahren?

Microsoft speichert die Daten georedundant an mehreren Stellen in zwei verschiedenen Rechenzentren. Dementsprechend sind zur Wiederherstellung bei Datenverlust keine Back-ups erforderlich. Sofern der Kunde eine Wiedergabe von historischen Datenständen benötigt, muss er zusätzlich zum Microsoft Cloud Service eine Archivierungslösung einsetzen.

Welche sonstigen regulatorischen Anforderungen können neben dem Datenschutzrecht zum Tragen kommen?
Die Anforderungen können hier nicht abschließend aufgezählt werden. In der Praxis können beispielsweise sektorspezifische Anforderungen wie im Finanzdienstleistungsbereich einschlägig sein. Nach den allgemeinen handels- und steuerrechtlichen Grundsätzen zur Buchführung bedarf es insbesondere der Einhaltung einer ordnungsgemäßen Behandlung elektronischer Dokumente (GoBS). Wesentlicher Kernpunkt ist hierbei das sogenannte „Interne Kontrollsystem" (IKS). Zum Nachweis eines funktionierenden IKS, welches Unternehmen gefährdende Entwicklungen frühzeitig erkennt, bietet Microsoft dem Kunden bzw. dessen Wirtschaftsprüfer eine Zertifizierung nach dem international anerkannten Prüfungsstandard ISAE 3402 an.

Weitere aktuelle Informationen finden Sie hier:

- Office 365 Trustcenter
  http://trust.office365.de

- Häufig gestellte Fragen zur Richtlinientreue in Office 365
  http://office.microsoft.com/de-de/business/redir/XT104103721.aspx

- Häufig gestellte Fragen zu den Standardvertragsklauseln der EU
  http://office.microsoft.com/de-de/business/redir/FX104033856.aspx

- Datenzugriff durch Dritte
  http://office.microsoft.com/de-de/business/redir/XT103403445.aspx

- Standorte der Rechenzentren
  http://office.microsoft.com/de-de/business/redir/XT103403404.aspx

- Verwaltungszugriff
  http://office.microsoft.com/de-de/business/redir/XT103403417.aspx

- Blogs zu der aktuellen Debatte zu NSA:
  http://blogs.technet.com/b/microsoft_blog/archive/2013/12/04/protecting-customer-data-from-government-snooping.aspx

  http://blogs.technet.com/b/microsoft_on_the_issues/archive/2014/02/03/providing-additional-transparency-on-us-government-requests-for-customer-data.aspx

- Microsoft veranstaltet in regelmäßigen Abständen Cloud Workshops mit einem Schwerpunkt in Bezug auf rechtliche Themen. Diese werden unter folgender Internetadresse angekündigt: **www.mscloudevent.de.**